3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden:

APP.4.2.A1 Sichere Konfiguration des SAP-ABAP-Stacks (B)

Der SAP-ABAP-Stack MUSS sicher konfiguriert werden. Dazu MÜSSEN die jeweiligen Profilparameter gesetzt werden, z. B. für die Passwortsicherheit, Authentisierung und Verschlüsselung. Auch MÜSSEN die Systemänderbarkeit und die Mandanten konfiguriert, das IMG-Customizing durchgeführt und die Betriebssystemkommandos abgesichert werden.

APP.4.2.A2 Sichere Konfiguration des SAP-JAVA-Stacks (B)

Der SAP-JAVA-Stack MUSS sicher konfiguriert werden, falls dieser eingesetzt wird. Dafür MÜSSEN andere Sicherheitsmechanismen und -konzepte erstellt werden als für den SAP-ABAP-Stack. Deshalb MÜSSEN Administrierende die Architektur des JAVA-Stacks kennen und wissen, wie er administriert wird. Zudem MÜSSEN nicht benötigte Dienste abgeschaltet, Standardinhalte entfernt, HTTP-Dienste geschützt und Zugriffe auf Administrationsschnittstellen eingeschränkt werden.

APP.4.2.A3 Netzsicherheit (B)

Um die Netzsicherheit zu gewährleisten, MÜSSEN entsprechende Konzepte unter Berücksichtigung des SAP-ERP-Systems erstellt und Einstellungen am System durchgeführt werden.

Weiterhin SOLLTEN der SAP-Router und SAP Web Dispatcher eingesetzt werden, um ein sicheres SAP-Netz zu implementieren und aufrechtzuerhalten.

Um Sicherheitslücken aufgrund von Fehlinterpretationen oder Missverständnissen zu vermeiden, MÜSSEN sich die Bereiche IT-Betrieb, Firewall-Betrieb, Portalbetrieb und SAP-Betrieb miteinander abstimmen.

APP.4.2.A4 Absicherung der ausgelieferten SAP-Standard-Konten (B)

Direkt nach der Installation eines SAP-ERP-Systems MÜSSEN die voreingestellten Passwörter der SAP-Standard-Konten geändert werden. Auch MÜSSEN die eingerichteten SAP-Standard-Konten mithilfe geeigneter Maßnahmen abgesichert werden. Bestimmte SAP-Standard-Konten DÜRFEN NICHT benutzt werden, z. B. für RFC-Verbindungen und Background-Jobs.

APP.4.2.A5 Konfiguration und Absicherung der SAP-Konten-Verwaltung (B)

Die SAP-Konten-Verwaltung für ABAP-Systeme MUSS sorgfältig und sicher administriert werden. Aktivitäten, wie Konten anlegen, ändern und löschen, Passwörter zurücksetzen und entsperren sowie Rollen und Profile zuordnen, MÜSSEN zu den Aufgaben der Konto-Administration gehören.

APP.4.2.A6 Erstellung und Umsetzung eines Konten- und Berechtigungskonzeptes (B) [Fachabteilung, Entwickelnde]

Für SAP-ERP-Systeme MUSS ein Konten- und Berechtigungskonzept ausgearbeitet und umgesetzt werden. Dabei MÜSSEN folgende Punkte berücksichtigt werden:

- Identitätsprinzip, Minimalprinzip, Stellenprinzip, Belegprinzip der Buchhaltung, Belegprinzip der Berechtigungsverwaltung, Funktionstrennungsprinzip (Segregation of Duties, SoD), Genehmigungsprinzip, Standardprinzip, Schriftformprinzip und Kontrollprinzip MÜSSEN berücksichtigt werden.
- Konto-, Berechtigungs- und gegebenenfalls Profiladministrierender MÜSSEN getrennte Verantwortlichkeiten und damit Berechtigungen haben.
- Vorgehensweisen im Rahmen der Berechtigungsadministration für *Rollen anlegen, ändern, löschen, transportieren und SU24 Vorschlagswerte transportieren* MÜSSEN definiert werden. Dabei SOLLTEN Berechtigungsrollen nur im Entwicklungssystem angelegt und gepflegt werden. Sie SOLLTEN mit Hilfe des Transport-Management-Systems (TMS) transportiert werden. Berechtigungen SOLLTEN in Berechtigungsrollen (PFCG-Rollen) angelegt, gespeichert und den Konten zugeordnet werden (rollenbasiertes Berechtigungskonzept). Da sich einzelne kritische Aktionen in den Rollen nicht immer vermeiden lassen, SOLLTEN sie von kompensierenden Kontrollen (mitigation controls) abgedeckt werden.

- Vorgehensweisen im Rahmen der Berechtigungsvergabe für *Konten und Berechtigungen beantragen, genehmigen, ändern und löschen* MÜSSEN definiert werden.
- Namenskonventionen für Konten-Kennungen und technische Rollennamen MÜSSEN definiert werden.
- Vorschlagswerte und Prüfkennzeichen SOLLTEN in der Transaktion SU24 gepflegt werden. Die Vorgehensweise dazu SOLLTE im Konten- und Berechtigungskonzept beschrieben sein.
- Gesetzliche und interne Rahmenbedingungen wie die Grundsätze ordnungsgemäßer Buchführung (GoB), das Handelsgesetzbuch (HGB) oder interne Vorgaben der Institution MÜSSEN berücksichtigt werden. Das Konten- und Berechtigungskonzept SOLLTE auch den Betrieb technischer Konten abdecken, also auch die Berechtigung von Hintergrund- und Schnittstellenkonten.

Es SOLLTEN geeignete Kontrollmechanismen angewandt werden, um SoD-Konfliktfreiheit von Rollen und die Vergabe von kritischen Berechtigungen an Konten zu überwachen.

Werden neben dem ABAP-Backend weitere Komponenten wie SAP HANA und SAP NetWeaver Gateway (für Fiori-Anwendungen) verwendet, MUSS das Design der Berechtigungen zwischen den Komponenten abgestimmt und synchronisiert werden.

APP.4.2.A7 Absicherung der SAP-Datenbanken (B)

Der Zugriff auf SAP-Datenbanken MUSS abgesichert werden. Administrierende SOLLTEN möglichst nur mit SAP-Tools auf die Datenbanken zugreifen können. Wird dazu Software von fremden Institutionen benutzt, MÜSSEN zusätzliche Sicherheitsmaßnahmen umgesetzt werden. Es DARF dann kein Schema-Konto des SAP Systems für die Verbindung zur Datenbank genutzt werden. Außerdem MÜSSEN Standardpasswörter geändert und bestimmte Datenbanktabellen (z. B. USR* Tabellen) besonders geschützt werden.

APP.4.2.A8 Absicherung der SAP-RFC-Schnittstelle (B)

Zum Schutz der Remote-Function-Call (RFC)-Schnittstelle MÜSSEN RFC-Verbindungen, RFC-Berechtigungen und die RFC-Gateways sicher konfiguriert werden.

Es MÜSSEN für alle RFC-Verbindungen einheitliche Verwaltungsrichtlinien erstellt und umgesetzt werden. Dazu SOLLTEN die benötigten RFC-Verbindungen definiert und dokumentiert werden. Verbindungen mit hinterlegtem Passwort SOLLTEN nicht von niedriger privilegierten auf höher privilegierte Systeme (z. B. von *Dev* nach *Prod*) konfiguriert sein. Nicht mehr benutzte RFC-Verbindungen MÜSSEN gelöscht werden.

Alle RFC-Gateways MÜSSEN sicher administriert werden. Dazu MÜSSEN geeignete Profilparameter gesetzt werden, z. B. *gw/monitor, gw/reg_no_conn_info* und *snc/permit_insecure_start*. Alle Verbindungen über ein Gateway MÜSSEN unter dem Sicherheitsaspekt analysiert und bewertet werden. Außerdem MUSS die Protokollierung aktiv sein. Es MÜSSEN Zugriffssteuerungslisten (ACLs) definiert werden.

APP.4.2.A9 Absicherung und Überwachung des Message-Servers (B)

Der Message-Server MUSS durch geeignete Einstellungen in den Profilparametern abgesichert werden. Es MUSS unter anderem entschieden werden, ob für den internen Message-Server noch ACLs aufgebaut werden. Der Message-Server MUSS mithilfe von geeigneten Mechanismen überwacht werden, damit z. B. Systemausfälle des Message-Servers schnell erkannt werden.

APP.4.2.A10 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.4.2.A11 Sichere Installation eines SAP-ERP-Systems (S)

Bei der Installation eines SAP-ERP-Systems SOLLTEN aktuelle SAP-Sicherheitsleitfäden und -Dokumentationen berücksichtigt werden. Außerdem SOLLTEN die Sicherheitsrichtlinien der Institution eingehalten werden. Ebenso SOLLTE gewährleistet sein, dass das SAP-ERP-System auf einem abgesicherten Betriebssystem installiert wird.

APP.4.2.A12 SAP-Berechtigungsentwicklung (S) [Fachabteilung, Entwickelnde]

Die technischen Berechtigungen SOLLTEN aufgrund fachlicher Vorgaben entwickelt werden. Des Weiteren SOLLTEN SAP-Berechtigungen auf dem Entwicklungssystem der SAP-Landschaft angepasst oder neu erstellt werden. Das SOLLTE auch bei S/4HANA die Berechtigungsentwicklung auf HANA-Datenbanken mit einschließen. Hier SOLLTEN Repository-Rollen aufgebaut und transportiert werden. Datenbankprivilegien SOLLTEN NICHT direkt an Konten vergeben werden.

Bei Eigenentwicklungen für z. B. Transaktionen oder Berechtigungsobjekte SOLLTE die Transaktion SU24 gepflegt werden (Zuordnungen von Berechtigungsobjekten zu Transaktionen). Die Gesamtberechtigung * oder Intervalle in Objektausprägungen SOLLTEN vermieden werden.

Die Berechtigungsentwicklung SOLLTE im Rahmen eines Änderungsmanagements durchgeführt werden.

Es SOLLTE sichergestellt sein, dass das Produktivsystem ausreichend vor Berechtigungsänderungen geschützt ist und keine Entwicklerschlüssel vergeben werden. Das Qualitätssicherungssystem SOLLTE bei der Berechtigungsvergabe und ergänzenden Einstellungen analog zum Produktivsystem betrieben werden.

APP.4.2.A13 SAP-Passwortsicherheit (S)

Um eine sichere Anmeldung am SAP-ERP-System zu gewährleisten, SOLLTEN Profilparameter, Customizing-Schalter oder Sicherheitsrichtlinien geeignet eingestellt werden.

Die eingesetzten Hash-Algorithmen für die gespeicherten Hashwerte der Passwörter in einem SAP-ERP-System SOLLTEN den aktuellen Sicherheitsstandards entsprechen. Zugriffe auf Tabellen mit Hashwerten SOLLTEN eingeschränkt werden.

APP.4.2.A14 Identifizierung kritischer SAP-Berechtigungen (S) [Fachabteilung]

Der Umgang mit kritischen Berechtigungen SOLLTE streng kontrolliert werden. Es SOLLTE darauf geachtet werden, dass diese Berechtigungen, Rollen und Profile nur restriktiv vergeben werden. Dies SOLLTE auch für kritische Rollenkombinationen und additive Effekte wie z. B. Kreuzberechtigungen sichergestellt sein.

Kritische Berechtigungen SOLLTEN regelmäßig identifiziert, überprüft und bewertet werden. Die SAP-Profile *SAP_ALL* und *SAP_NEW** sowie das SAP-Berechtigungsobjekt *S_DEVELOP* (mit Änderungsberechtigungen *ACTVT 01* und *02*) SOLLTEN im Produktivsystem nicht vergeben werden. Notfall-Konten SOLLTEN von dieser Vorgabe ausgeschlossen sein.

APP.4.2.A15 Sichere Konfiguration des SAP-Routers (S)

Der SAP-Router SOLLTE den Zugang zum Netz regeln und die bestehende Firewall-Architektur zweckmäßig ergänzen. Auch SOLLTE er den Zugang zum SAP-ERP-System kontrollieren.

APP.4.2.A16 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows (S)

Das SAP-ERP-System SOLLTE NICHT auf einem Windows-Domaincontroller installiert werden. Die SAP-spezifischen Konten wie *<sid>adm* oder *SAPService <sid>* SOLLTEN abgesichert werden. Nach der Installation SOLLTE das Konto *<db><sid>* gesperrt werden.

Das Konto SAPService *<sid>* SOLLTE KEINE Rechte zur interaktiven Anmeldung besitzen. In Bezug auf diese Berechtigungen SOLLTEN die zum SAP-ERP-System dazugehörigen Systemressourcen wie Dateien, Prozesse und gemeinsam genutzte Speicher geschützt werden.

Die spezifischen Berechtigungen der vom SAP-ERP-System angelegten Konten *Guest, System, SAP system users = <sapsid>adm, SAPService<SAPSID>* und *Database users = <database-specific users>* und Benutzendengruppen SOLLTEN mithilfe geeigneter Einstellungen abgesichert werden.

APP.4.2.A17 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Unix (S)

Für die SAP-ERP-Systemverzeichnisse unter Unix SOLLTEN Zugriffsberechtigungen festgelegt werden. Auch SOLLTEN die Passwörter der systemspezifischen Konten *<sid>adm* und *<db><sid>* geändert werden. Nach der Installation SOLLTE das Konto *<db><sid>* gesperrt werden.

APP.4.2.A18 Abschaltung von unsicherer Kommunikation (S)

Die Kommunikation mit und zwischen SAP-ERP-Systemen SOLLTE mit SNC abgesichert werden. Sofern Datenbank und SAP-Applikationsserver auf verschiedenen Systemen betrieben werden, SOLLTE die Datenbankverbindung in geeigneter Weise verschlüsselt werden. Die internen Dienste des SAP-Applikationsservers SOLLTEN nur mittels TLS miteinander kommunizieren.

APP.4.2.A19 Definition der Sicherheitsrichtlinien für Konten (S)

Für die jeweiligen Konten und Kontengruppen SOLLTEN spezifische Sicherheitsrichtlinien für Passwörter und Anmelderestriktionen erstellt werden. So SOLLTEN beispielsweise Konten mit kritischen Berechtigungen durch starke Passwortregeln abgesichert sein (Transaktion SECPOL). Die Sicherheitsrichtlinien SOLLTEN den Konten korrekt zugeordnet und regelmäßig überprüft werden.

APP.4.2.A20 Sichere SAP-GUI-Einstellungen (S)

Die SAP GUI SOLLTE auf allen Clients installiert und regelmäßig aktualisiert werden. Auch SOLLTEN SAP GUI ACLs aktiviert sowie angemessene Administrationsregeln verteilt und aktiviert werden.

APP.4.2.A21 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.2.A22 Schutz des Spools im SAP-ERP-System (S) [Entwickelnde]

Es SOLLTE sichergestellt sein, dass auf Daten der sequenziellen Datenverarbeitung wie Spool oder Druck nur eingeschränkt zugegriffen werden kann. Auch SOLLTE verhindert werden, dass unberechtigte Konten auf die vom SAP-Spoolsystem benutzte Datenablage TemSe zugreifen können. Die hierfür vergebenen Berechtigungen SOLLTEN regelmäßig überprüft werden.

APP.4.2.A23 Schutz der SAP-Hintergrundverarbeitung (S) [Entwickelnde]

Die SAP-Hintergrundverarbeitung SOLLTE vor unberechtigten Zugriffen geschützt werden. Dafür SOLLTEN für Batch-Jobs verschiedene System-Konten nach ihren Funktionsbereichen definiert und angelegt werden. Der so genannte Benutzertyp Dialog SOLLTE dafür grundsätzlich NICHT zugelassen werden.

APP.4.2.A24 Aktivierung und Absicherung des Internet Communication Frameworks (S)

Es SOLLTE darauf geachtet werden, dass nur notwendige ICF-Dienste aktiviert werden. Alle ICF-Dienste, die unter einem ICF-Objekt sind, SOLLTEN nur einzeln aktiviert werden. ICF-Berechtigungen SOLLTEN restriktiv vergeben werden. Die Kommunikation SOLLTE verschlüsselt erfolgen.

APP.4.2.A25 Sichere Konfiguration des SAP Web Dispatchers (S)

Der SAP Web Dispatcher SOLLTE nicht der erste Einstiegspunkt aus dem Internet zum SAP-ERP-System sein. Der SAP Web Dispatcher SOLLTE auf dem aktuellen Stand sein. Er SOLLTE sicher konfiguriert sein.

APP.4.2.A26 Schutz von selbstentwickeltem Code im SAP-ERP-System (S)

Es SOLLTE ein Custom-Code-Managementprozess definiert werden, damit selbstentwickelter Code ausgetauscht oder entfernt wird, falls er durch SAP-Standard-Code ersetzt werden kann oder er nicht mehr benutzt wird. Ferner SOLLTEN die Anforderungen aus der Richtlinie für die Entwicklung von ABAP-Programmen berücksichtigt werden.

APP.4.2.A27 Audit des SAP-ERP-Systems (S) [Fachabteilung]

Damit sichergestellt ist, dass alle internen und externen Richtlinien sowie Vorgaben eingehalten werden, SOLLTEN alle SAP-ERP-Systeme regelmäßig auditiert werden. Dafür SOLLTE der Security Optimization Service im SAP Solution Manager benutzt werden. Die Ergebnisse des Audits SOLLTEN ausgewertet und dokumentiert werden.

APP.4.2.A28 Erstellung eines Notfallkonzeptes (S) [Notfallbeauftragte]

Für SAP-ERP-Systeme SOLLTE ein Notfallkonzept erstellt und betrieben werden. Es SOLLTE die Geschäftsaktivitäten absichern und mit den Vorgaben aus dem Krisenmanagement oder dem Business-Continuity-Management übereinstimmen. Im Notfallkonzept SOLLTEN folgende Punkte beschrieben und definiert werden:

- Detektion von und Reaktion auf Zwischenfälle,
- Datensicherungs- und Wiederherstellungskonzept sowie
- Notfalladministration.

Das Notfallkonzept SOLLTE regelmäßig aktualisiert werden.

APP.4.2.A29 Einrichten von Notfall-Konten (S)

Es SOLLTEN Notfall-Konten angelegt werden. Die eingerichteten Konten und Berechtigungen SOLLTEN stark kontrolliert und genau dokumentiert werden. Außerdem SOLLTEN alle von Notfall-Konten durchgeführten Aktivitäten protokolliert werden.

APP.4.2.A30 Implementierung eines kontinuierlichen Monitorings der Sicherheitseinstellungen (S)

Es SOLLTE ständig überwacht werden, ob alle Sicherheitseinstellungen des SAP-ERP-Systems korrekt sind. Außerdem SOLLTE überwacht werden, ob alle Patches und Updates ordnungsgemäß eingespielt wurden. Das SAP-Monitoring SOLLTE in die allgemeine Systemüberwachung der Institution integriert werden.

APP.4.2.A31 Konfiguration von SAP Single-Sign-On (S)

Sind mehrere SAP-ERP-Systeme vorhanden, SOLLTEN die Benutzenden auf die Systeme mit SAP Single-Sign-On (SAP SSO) zugreifen. Es SOLLTE in der Planungsphase entschieden werden, zwischen welchen SAP-ERP-Systemen der SSO-Mechanismus benutzt wird. Das SSO SOLLTE sicher konfiguriert und betrieben werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.4.2.A32 Echtzeiterfassung und Alarmierung von irregulären Vorgängen (H)

Die wichtigsten Sicherheitsaufzeichnungsfunktionen der SAP-ERP-Systeme wie Security Audit Log oder System Log SOLLTEN kontinuierlich überwacht werden. Bei verdächtigen Vorgängen SOLLTEN automatisch die zuständigen Mitarbeitenden alarmiert werden. Um SAP-spezifische Sicherheitsvorfälle analysieren und Falschmeldungen von echten Sicherheitsvorfällen abgrenzen zu können, SOLLTEN entweder Mitarbeitende geschult oder entsprechende Serviceleistungen von Drittanbietenden genutzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das SAP Help Portal (https://www.help.sap.com/viewer/index) ist der zentrale Einstieg in die SAP Hilfe. Sie bietet zu vielfältigen Themen umfangreiche Informationen und Anleitungen. Im Folgenden wird eine Auswahl an Themen, die im Kontext SAP-ERP-Systeme interessant sind, aufgelistet:

- SAP Audit Management, https://help.sap.com/saphelp_fra110/helpdata/de/ab/ce1b52bd543c3ae10000000a441470/frameset.htm und https://help.sap.com/saphel_erp60_sp/helpdata/de/f9/558f40f3b19920e10000000a1550b0/content.htm
- Benutzerverwaltung mit AS Java, https://help.sap.com/saphelp_nw73/helpdata/de/45/b90177cf2252f8e10000000a1553f7/content.htm?no_cache=true
- Zentrale Benutzerverwaltung (ZBV), https://help.sap.com/doc/erp2005_ehp_07/6.07/de-DE/8d/270bea613d2443bad6ce0524f08ca0/frameset.htm

Detaillierte Best-Practice-Empfehlungen für die Prüfungen von SAP-ERP-Systemen, bietet der Prüfleitfaden SAP ERP 6.0: Best Practice – Empfehlungen der Deutschsprachigen SAP Anwendergruppe e. V. (DSAG).